Mangalore University

Pre-Synopsis

of the PhD Thesis to be submitted for the award of the degree of

Doctor of Philosophy in

Computer Science

Title of the Work

MACHINE LEARNING ALGORITHMS FOR DIGITAL MEDIA FORGERY DETECTION

By

Wincy Abraham,

Research Scholar

Under the Guidance of

Dr. B.H. Shekar,

Professor

Department of Post-Graduate Studies and Research in Computer Science,

Mangalore University,

Mangalagangotri-574 199

APRIL 2024

Contents

1 Introduction **1**

1.1 Image Forgery 2

1.2 Video Forgery 3

2 Image Forgery Detection using Discrete Cosine Transform **4**

2.1 Proposed Image Forgery Detection Technique using Local DCT Features . 5

2.2 Experimental Results and Discussion 6

2.2.1 Datasets 6

2.2.2 Evaluation Metrics 7

3 Image Forgery Detection and Localization using Recompression based Approach **7**

3.1 Proposed Image Forgery Detection using Recompression based Approach . 8

3.1.1 Experimental Results and Discussion 9

3.2 Proposed Image Forgery Localization using Recompression 10

3.2.1 Experimental Results and Discussion 12

4 Inter-Frame Video Forgery Detection and Localization in Spatial Domain **13**

4.1 Proposed Inter-Frame Video Forgery Detection and Localization by Pixel Based Statistical Analysis 13

4.1.1 Experimental Results and Discussion 15

4.2 Proposed Inter-Frame Video Forgery Detection and Localization using Principal Component Analysis 17

4.2.1 Experimental Results and Discussion 20

5 Contributions of this Research Work **20**

6 Conclusion **22**

MACHINE LEARNING ALGORITHMS FOR DIGITAL MEDIA FORGERY DETECTION

1 Introduction

Digital media encompasses a broad spectrum of content, information, and communication that is produced and distributed in electronic formats. It manifests in various forms, including text, images, audio, and video. The advent of digital media has revolutionized communication, enabling real-time interaction, global connectivity, and the rapid dissemination of information. It has empowered individuals to create and share content easily, fostering a democratization of media production. Social media platforms, online streaming services, and digital publications have become integral to daily life, shaping how people connect, access news, and entertain themselves. Thus digital media has now become so important in the daily activities of a person that now we can not think of a scenario deprived of it.

However, the digital media platform also presents challenges, including issues related to privacy, security, misinformation, and digital manipulation. As technology continues to evolve, so does the complexity of comprehending digital media content. Understanding the dynamics of digital media is crucial for individuals, businesses, and societies to harness its benefits while addressing its challenges responsibly. The consequences of digital image manipulation are far-reaching and impact various domains, including journalism, forensics, and social media. It poses challenges to the authenticity and integrity of visual information, leading to concerns about the spread of misinformation and the erosion of trust in digital content.

Detecting and preventing digital image forgery involves the development of advanced forensic techniques. There are many forgery detection methods developed so far but none is fool-proof. The above-mentioned challenges along with the need for powerful forgery detection tools motivated us to carry out research work that deals with the detection of forgery in digital media, especially image and video.

Figure 1: Authentic image

Figure 2: Copy-Move image

1.1 Image Forgery

Digital image forgery refers to the manipulation or alteration of digital images with the intent to deceive, mislead, or create a false representation of reality. As digital imaging technologies have become more sophisticated and widely accessible, the potential for image forgery has increased significantly. This practice involves the use of various tools and techniques to modify the content of images, creating deceptive visuals that may be difficult to distinguish from authentic ones. Digital images may contain any type of information like a picture of a scene or event, hand-written document, signature, vehicle number plate, and anything of that sort.

A forger intentionally alters digital images to hide the evidence of crimes or for some illegal activity. This type of forgery can cause difficulty in proving crimes by the court of law or any other authority. Sometimes forgery is done to make false reports which may not cause any legal harm but hide the truth from the general public. Whatever be the intention behind forgery, it must be discouraged. Since the rate of image forgery is too high today, people cannot believe what they see, but apply some mechanism to check the genuineness before comprehending it. Genuine content is utilized and inauthentic matter is discarded.

Normally image forgery is done with many of the image editing tools in such a way that the image appears to be genuine or in other words forgery cannot be detected by the naked eye. Sometimes anti-forensic approaches are employed by forgers so that forgery detection becomes an unsuccessful task. Image forgery can be done by repositioning objects within the same image, copying and placing objects in other regions in the same image (copy-move) as in Figure.2 or by placing objects from other images (splicing) as shown in Figure.5. There are many challenges to image forgery detection attempts like advancements in forgery techniques, diverse types of forgeries, and the need for real-time detection for social media and news verification. However, some literature concentrates on specific forgery types, potentially overlooking the need for comprehensive models capable of detecting a range of manipulations within a single image. Also, the practicality of real-

Figure 3: Authentic image

Figure 4: Authentic image

Figure 5: Spliced image

time forgery detection is not always emphasized in current literature. Deployable solutions that balance accuracy and computational efficiency are crucial for real-world applications. In this research work, we proposed methods that could overcome some challenges like diverse types of forgeries and the need for real-time detection.

1.2 Video Forgery

Video forgery refers to the creation or alteration of video content with the intent to deceive or mislead viewers. As video editing tools and technologies have become more sophisticated and widely accessible, the potential for video forgery, including the creation of deepfakes, has increased significantly. Such manipulations of video content can serve various malicious purposes, including the dissemination of misinformation, propaganda, or the creation of false evidence. The widespread availability of video editing tools has significantly simplified the creation of deceptive video content and emphasized the increased demand for robust video forgery detection techniques.

Many methods in the literature for video forgery detection are found to be computationally intensive. Also, the absence of standardized benchmarks and evaluation metrics hinders the comparison of different video forgery detection methods. So, we are motivated to develop efficient video forgery detection techniques. As technology continues to evolve, staying vigilant and employing robust forgery detection methods is crucial to maintaining trust in digital video content and ensuring the integrity of information disseminated through video platforms.

The rest of this pre-synopsis is organised as follows. Image Forgery Detection using DCT is explained in sub-section 2.1 of Section 2. Image Forgery Detection and Localization using Recompression are discussed in sub-section 3.1 and in sub-section 3.2 of Section 3 respectively. Approaches proposed based on Spatial Intensity Variations and based on PCA of video frames, for Video Forgery Detection and Localization are explained in subsections 4.1 and 4.2 respectively. Details of the experiments, discussions on results and

comparative analysis are presented in the corresponding sections themselves. The Contributions of this work are presented in Section 5 and a summary and related publications are presented in Section 6 of this document.

2 Image Forgery Detection using Discrete Cosine Transform

The Discrete Cosine Transform(DCT) is a technique that converts a signal or image from its spatial domain into frequency domain. It is obtained using the equation

$$\mathrm{DCT}_{u,v} = \alpha(u)\alpha(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cos\left(\frac{(2x+1)u\pi}{2M}\right) \cos\left(\frac{(2y+1)v\pi}{2N}\right) \tag{1}$$

Here, $\mathrm{DCT}_{u,v}$ represents the DCT coefficient at frequency indices u and v, and f(x, y) is the pixel intensity at spatial coordinates (x, y). M and N are the dimensions of the 2D block, and $\alpha(u)$ and $\alpha(v)$ are scaling factors given by:

$$\alpha(x) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{if } x = 0 \\ 1, & \text{otherwise} \end{cases}$$

In the context of image and video compression, the DCT is applied to blocks of pixels, and the resulting coefficients emphasize the important frequency components of the image while discarding less important information. This helps in reducing the amount of data needed to represent the image or video, leading to efficient compression.

The primary objective of this approach using Discrete Cosine Transform is to identify alterations and manipulations within digital images by analyzing their frequency domain representation. DCT is commonly employed in image compression, and variations in the DCT coefficients can reveal anomalies introduced through forgery. The goal is to develop techniques that can effectively distinguish between authentic and manipulated images, providing a reliable means of detecting various types of forgeries. The proposed approach is capable of identifying any type of forgery.

There are several works carried out by researchers utilizing features based on the DCT of the image. Gani et.al. [5] proposed a robust technique for copy-move forgery detection based on sign information of local DCT and cellular automata. The k-d tree-based nearest neighbour matching method is used to find the duplicate areas in the image. Cao et al. [2] proposed a method in which DCT was performed on the fixed-size blocks of the image. To reduce the dimension of the feature vector, only four coefficients are taken from each block. Though it performs well on multiple copy-move forgery, noise and blur, there are problems

with false matches. Haiwei et.al [20] propose Forensic Contrastive Clustering (FOCAL), a novel simple and effective method using contrastive learning and clustering. It utilizes pixel-level contrastive learning for high-level forensic feature extraction. It also employs a clustering algorithm to group the features learned into authentic or forged. Further, it boosts the image forgery detection performance via simple feature-level concatenation without requiring retraining. Patel et.al [14] integrates Error Level Analysis with CNN for image forgery detection. Our efforts in this direction have resulted in the development of the following approach which effectively detects image forgery.

2.1 Proposed Image Forgery Detection Technique using Local DCT Features

This approach makes use of the variation in the local statistics of the block DCT coefficients (BDCT) of the image due to tampering, as an indication of the forgery. Local DCT features as explained in the article by Dua et al.[4] are explored. Initially, the image is converted to the YCbCr colour space and then three different channels Y, Cb and Cr are taken for further processing. The feature vector obtained for each channel is combined and then reshaped and fed to the deep neural network model(DNN) for forgery detection. A DNN model performs the classification of images.

The input image channel is first divided into non-overlapping 8X8 blocks and the DCT of each block is computed and stored column-wise in a matrix containing 64 rows. The number of columns in this matrix will be equal to the number of 8X8 blocks in the image. Next, the image is cropped by removing the first 4 rows and 4 columns and the above process is repeated. From the two matrices created which contain the DCT coefficients of all blocks column-wise, the standard deviation of the values in each row is found out except for the row corresponding to the DC coefficient. The number of non-zero coefficients is also found in each row except the first row. This results in an array of size $63X2$ containing the standard deviation and the number of non-zero DCT coefficients of the 63 rows in the matrix. Thus, there are two such arrays corresponding to the image and its cropped version. Next, these arrays are appended and treated as the feature vector. Figure.6 shows the structural outline of the proposed forensic detector based on DCT-domain features. These features are fed into a deep neural network model for the detection. This model using deep learning architecture is found to perform better than those using conventional machine learning models.

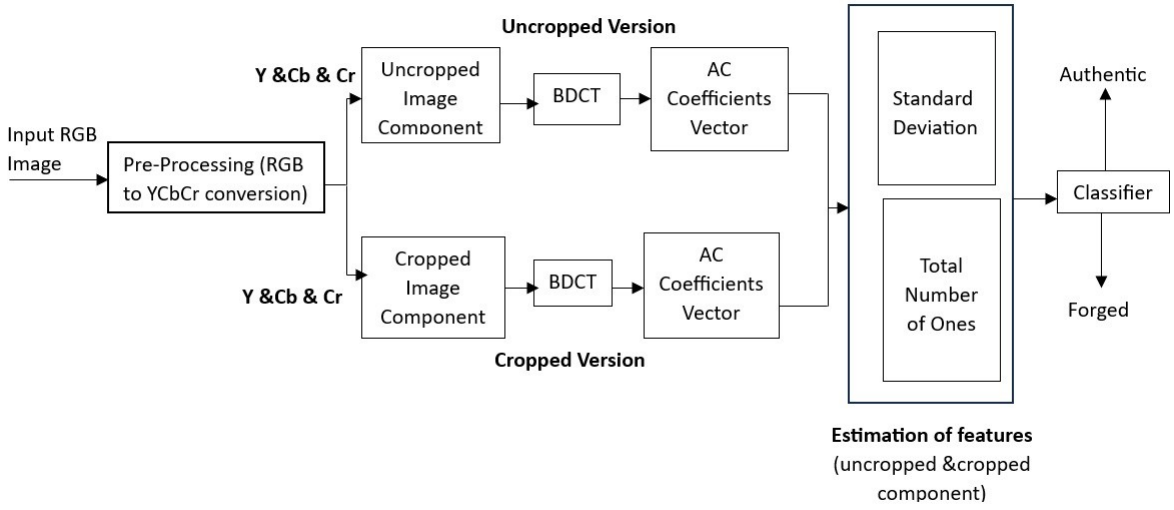

Figure 6: Block diagram of the DCT-based Image Forgery Detection

2.2 Experimental Results and Discussion

In this section, we describe the experimental analysis of the proposed approaches for image forgery detection. Publicly available datasets are collected based on the requirement for experimentation and preprocessing is applied to the data to make it ready for experimentation. The images underwent colour conversion to the YCbCr colour space for forgery detection using DCT.

2.2.1 Datasets

The technique proposed for Image Forgery Detection has been extensively tested using publicly available datasets CASIA 1 and CASIA 2[3] constructed by the Institute of Automation Chinese Academy of Sciences which is considered to be more challenging and realistic dataset for manipulation detection. In CASIA 1, there is a total of 1721 images in which 800 images are authentic and 921 images are tampered colour images of size 384×256 and all are in JPEG format without any post-processing. On the other hand, CASIA 2 consists of multiple sized images with various post-processing applied across edges. CASIA 2 consists of 7491 authentic and 5123 forged colour images with size varying from 240×160 to 900×600 pixels. Also, the images are available as uncompressed as well as in JPEG format with different quality factors.

Table 1: Comparitive analysis of Image Forgery Detection using Local DCT Features in terms of Accuracy(%)

Approach	**CASIA 1**	**CASIA 2**
Ali et.al[1]	-	92.23
Dua et.al[4]	93.2	98.3
Vidyadharan et.al[18]	94.13	97.03
Proposed Local DCT-based	95.08	97.56

2.2.2 Evaluation Metrics

The metric used for performance evaluation for image forgery detection is Accuracy. Accuracy is a measure of the correctness of a classification model. It is calculated as

$$\text{Accuracy} = \frac{\text{Number of Correct Predictions}}{\text{Total Number of Predictions}} \tag{2}$$

We have conducted experimentation using the datasets described in 2.2.1. Feature vectors are extracted from the input images and they are fed to the DNN and the performance metrics are calculated. Adam optimizer with a learning rate of 0.001 is used. Initial decay rates, beta1 = 0.9 and beta2 = 0.999 are used. The exponential decay parameter is set as 0.0001 with an epsilon value of 1e-08. The DNN is trained using 80% of the data with a batch size of 10. Table 1 shows the comparative analysis of the proposed approach. It confirms that the proposed approach outperforms some of the well-known methods in the state-of-the-art.

3 Image Forgery Detection and Localization using Recompression based Approach

JPEG compression is a lossy compression method which is employed in most of the image-capturing devices. When the image is saved again in JPEG format, the same compression is repeated. This is called double compression. Usually, the quality factor used in re-compression will be different from the one used in initial compression. Almost all images have undergone at least a single compression, during the image capture as most cameras use jpeg compression while saving the images. The compression artefacts are analysed

by the proposed techniques to detect and localize forgery. The forgery detection method using recompression is fast and efficient and can perform real-time detection of any type of forgery.

The objective of image forgery detection and localization using recompression is to identify instances of manipulation or tampering within digital images by analyzing the artefacts introduced during the recompression process. Recompression involves compressing an already compressed image, leading to changes in compression artefacts.

Several works in the state-of-the-art literature use compression artefacts present in the image for forgery detection and localization. Luo et.al[11] use error-level analysis for image forgery detection. The rounding error and truncation error happening during JPEG compression are analyzed and used to detect double compression and quantization table used in compression. Syed et.al.[1] proposed a method in which the difference between the original and recompressed image is used as a feature to train a CNN which can detect forgery by the compression artefacts in the image. Hao et.al.[7] use a novel image forgery localization method using transformers. They use dense self-attention encoders and dense correction modules as major components in their model.

In the proposed approaches we use the discrepancies in the compression artefacts to detect and localize image forgery. Our goal is to design techniques that can effectively detect compression artefacts and reveal inconsistencies in the compression history of an image, thereby indicating potential forgery.

3.1 Proposed Image Forgery Detection using Recompression based Approach

The approach proposed here for Image Forgery Detection uses techniques that extract compression artefacts to detect forgery effectively. The artefacts emerging in lossy compression are extracted by recompression. When a JPEG image is altered by copy-move or splicing, the original pixel intensities get modified with new values at the location of forgery causing a change in the 8X8 DCT block structure created for compression when the image was first saved. When the image is saved after modification, the coefficients corresponding to the original parts of the image remain the same after compression while the altered region will have their coefficients changed. This change becomes visible when the image is compressed again especially when the recompression is done using the same quality level as the one used by the original image (Selective recompression). It means that if the image is authentic, the original image and its recompressed version will not have much difference while the forged image and its recompressed version exhibit signifi-

cant differences. The extent of change in the original and recompressed images varies with varying quality levels of recompression. The change is minimal when the quality factor is the same as that used in the initial compression of the major portion of the image. The same change is exhibited in the histograms of the original and recompressed images at different quality levels.

In the proposed approach, the compression artefacts occurring in the JPEG images in various forms are used as feature vectors to detect forgery. This idea is used in the construction of three different feature vectors for image forgery detection. The block diagram depicting the classification is shown in Figure.7. The feature vector for classification

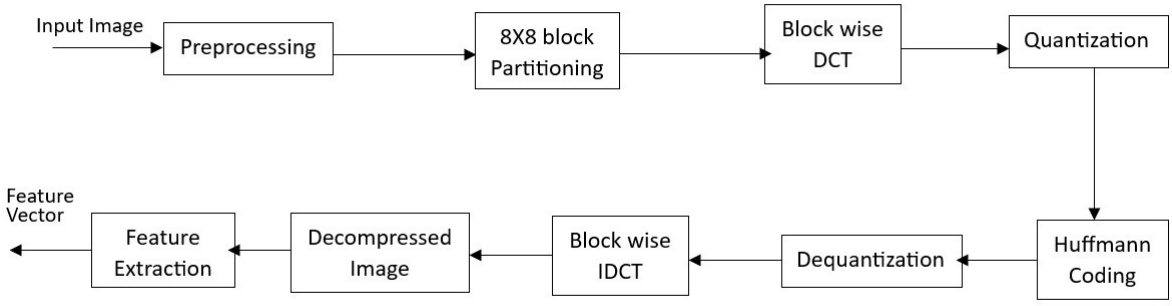

Figure 7: Block diagram illustrating the Recompression-based Forgery Detector

consists of these three components.

- Sum of the difference in values in the original and recompressed image array.
- Sum of the minimal difference in values in the original and recompressed image array.
- Standard deviation of Block-wise difference in the histogram bin edges of the original and recompressed image.

The feature vectors are fed to the Support Vector Machine classifier which detects whether the image is authentic or forged.

3.1.1 Experimental Results and Discussion

Publicly available datasets are collected based on the requirement for experimentation and preprocessing is applied to the data to make it ready for experimentation. The images underwent grayscale conversion for forgery detection using the recompression technique.

Table 2: Comparative Analysis of Image Forgery Detection using Recompression-based Approach in terms of Accuracy(%)

Approach	**CASIA 1**	**CASIA 2**
Patankar et.al[13]	-	95.19
Dua et.al[4]	93.2	98.3
Vidyadharan et.al[18]	94.13	97.03
Proposed Recompression-based	97.1	91.31

Recompression-based method for Image Forgery Detection has been extensively tested using publicly available datasets CASIA 1 and CASIA 2 which are described in section 2.2.1. The evaluation metric used is Accuracy which is described in section 2.2.2. For all the images in the datasets, feature vectors are extracted. For training the classifier 80% of the feature vectors from the dataset are used and the remaining 20% is used for testing. SVM classifier is used for the classification of images as authentic or tampered. Table 2 contains the results. The proposed method is found to give higher accuracy compared to the state-of-the-art methods.

It is seen that the proposed approaches for Image Forgery Detection described in sections 2.1 and 3.1 outperform state-of-the-art methods. The result for image forgery detection using recompression indicates that our approach improves the accuracy for the CASIA 1 dataset but not CASIA 2. A reason is that most of the images in CASIA 2 have undergone double compression which causes it not to provide the features necessary for accurate detection.

3.2 Proposed Image Forgery Localization using Recompression

Image forgery localization involves identifying regions in an image that have been tampered with or manipulated. Recompression analysis is one of the techniques used for detecting and localizing such forgeries. Recompression occurs when an image is saved or compressed multiple times using different compression algorithms or settings. Each compression step leaves a unique signature in the image data.

The concept of double compression is primarily associated with lossy compression formats, such as JPEG. On the other hand, TIFF (Tagged Image File Format) and PNG (Portable Network Graphics) are typically lossless compression formats. In these formats, compres-

sion is applied without discarding image information, and the image can be decompressed to its original form without loss. In the proposed work the degree of loss of image detail in JPEG compression is used for detecting and localizing image forgery. Since a forged image contains regions compressed at different quality levels, Selective Recompression helps in extracting the features needed for forgery localization. In Selective Recompression the image is recompressed with the same quality level as the one used in its initial compression and hence the loss in image detail due to recompression will be small. But if the image is forged, it will contain regions compressed at different quality levels. Then Selective Recompression will be using the quality level used by the major portion of the image. So, the region initially compressed at a different quality level will experience more degradation during the recompression process. This is because the compression algorithm will treat the region differently, potentially leading to more noticeable artefacts and loss of detail. This idea is used in this method to detect and localize forgery. A block diagram depicting the process is shown in Figure.8

Thresholding the difference between the original image and the image after selective

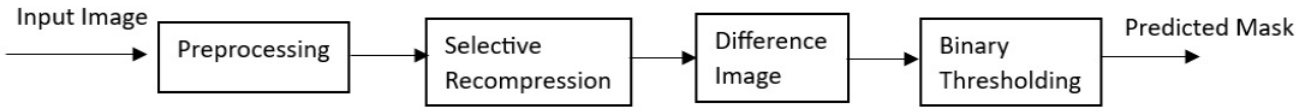

Figure 8: Block Diagram of the Forgery Localization Method

recompression yields the tampered region mask, as the quality level used for selective recompression is the same as the quality level used for the authentic region of the image in its initial compression. It is noteworthy that this method works better for most of the images saved in lossless compression formats like TIFF and PNG while the performance of JPEG images under this method depends on the quality level used in double compression and the initial compressions. Figure.9 shows the predicted masks for images from the datasets used in the experimentation. The proposed method is found to localize forgery effectively.

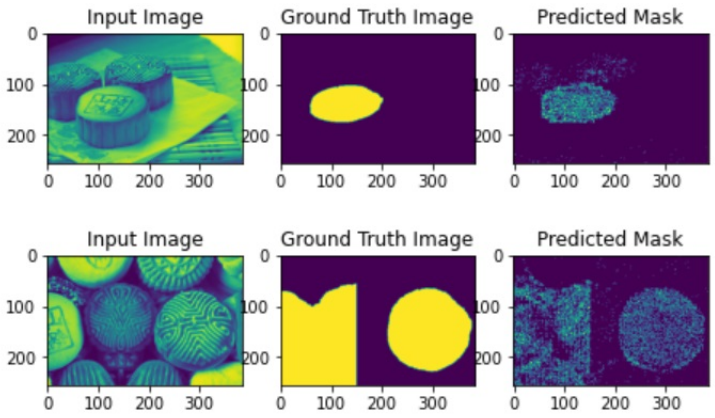

Figure 9: CASIA-Predicted Mask

3.2.1 Experimental Results and Discussion

In this section, we describe the experimental analysis of the proposed approach for image forgery localization. Datasets CASIA 1 and CASIA 2 with ground truth[15] which are publicly available are used in the experimentation. In CASIA 1 there are 921 forged images with ground truth information. In CASIA 2 there are 1828 spliced, and 3295 copy-move colour images with various sizes from 240×160 to 900×600 pixels. Only the non-JPEG images are considered from CASIA 2 for experimentation. The images underwent grayscale conversion for forgery localization using the recompression technique.

Performance metric used for image forgery localization is pixel level F1-score which weights each pixel equally, and a perfect score is only possible if all pixels are classified correctly as either mask or nonmask. The pixel-level F1 score is calculated using the following formula.

$$\text{F1 score} = \frac{2 \times \text{TP}}{2 \times \text{TP} + \text{FP} + \text{FN}} \tag{3}$$

where, *TP is the number of True Positives*, *FP is the number of False Positives*, *FN is the number of False Negatives*

The proposed approach is tested using the above datasets and the performance measured using the F1 score computation. It is found to perform well for image forgery localization by taking the compression artefacts into consideration. This approach works good for images which have undergone jpeg compression. It is found to work well for other image formats as well, as all images are supposed to undergo compression during image capturing since most cameras use jpeg compression using image capture. A comparison with the state-of-the-art methods is provided in Table 3. It is found to give comparable accuracy with those of the state-of-the-art.

Table 3: Comparitive Analysis of Image Forgery Localization using Recompression for CASIA Dataset

Approach	**F1 Score**
Hao et.al[7]	0.479
Han et.al[21]	0.361
Proposed Recompression-based	0.369

4 Inter-Frame Video Forgery Detection and Localization in Spatial Domain

Similar to images, videos can be processed in either the Spatial Domain or the Frequency Domain. Our emphasis is on Spatial Domain operations for detecting and localizing video forgeries. A forger may modify a video causing inter-frame forgery or intra-frame forgery. In intra-frame forgery, the manipulation takes place within a frame of the video. Some objects may be added or removed in the frame. Inter-Frame forgery causes alteration between two frames of the video. Some frames may be inserted in between two frames or removed from the video. An example of inter-frame forgery is frame duplication forgery where a set of frames within the video is copied or duplicated to another region in the video as shown in Figure.10.

For inter-frame forgery detection, there exist methods that make use of several features of the video like motion vector, coefficient of correlation between adjacent frames of the video, etc. Soumya et.al [19] use frame similarity analysis to locate inter-frame forgery due to frame replication. Wang et.al.[6] use correlation coefficient as a measure of similarity to find frame duplication. The similarity in the spatial and temporal correlations is used as an indication of frame duplication. Vinay et.al [10] find the inter-frame correlation distance between the frames, sets the appropriate threshold using statistical analysis using the minimum distance score for the detection and localization of image forgery. It detects insertion and deletion forgeries by using parameters controlled by threshold and is evaluated on the VIFFD dataset.

4.1 Proposed Inter-Frame Video Forgery Detection and Localization by Pixel Based Statistical Analysis

Spatial Intensity Variations provide valid clues regarding the authenticity of digital videos. The fact that adjacent frames do have continuous intensity distribution and any change in it is only due to the insertion or deletion of frames or by frame duplication, is used here.

Pixel intensity values of the corresponding pixels in the consecutive frames in the video will

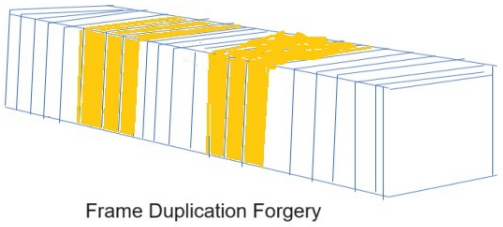

Figure 10: Frame Duplication

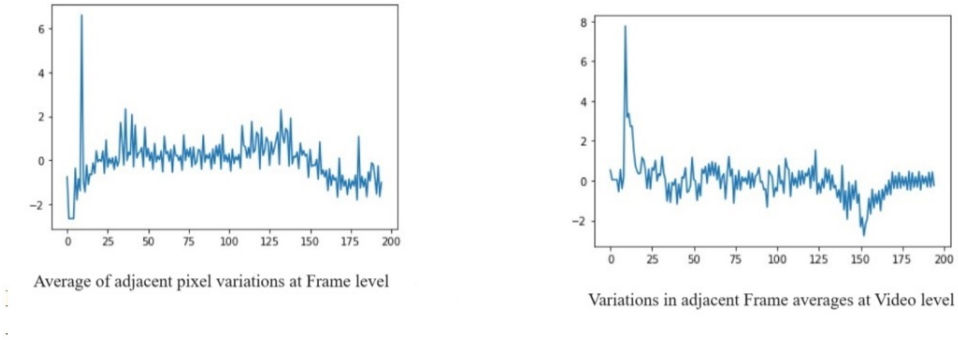

Figure 11: Pixel based Statistical Analysis

have small differences in most cases. Similar is the case with the correlation coefficient of adjacent frames. This fact is made use of in finding the inter-frame forgery. And this is true when there is no sudden scene change. If there are scene changes in the video, it will result in frames with varying content. The variation of content in adjacent frames may be due to camera motion, movement of objects within the scene, noise and change in lighting [9]. In the case of videos captured using surveillance cameras, camera motion problems will not be present. The difference caused by noise and change in lighting can be neglected as it will be small compared to the difference caused by moving objects. Thus the main cause of scene change when the video is captured using surveillance cameras is the movement of objects. But in videos with high frame rate, the change in adjacent frame intensities due to forgery outweigh the change due to object motion. However, the proposed approach performs better for videos with no sudden scene change. for the clue for forgery as the difference will be high if any frame under consideration is a newly inserted one or one which became adjacent due to the deletion of some frames in between as seen in Figure.11. Hence the feature vectors based on the pixel intensity in the adjacent frames are combined for forgery detection. The two arrays A_1 and A_2 used in this approach are computed as follows.

1. Difference Array D is found by finding the difference in intensity of each pixel in the adjacent frames as

$$D_k[i,j] = f_k[i,j] - f_{k+1}[i,j] \tag{7}$$

where k = 1 to n-1, where n is the total number of frames in the video, and i, j take values

as per the size of each frame.

A_1, the average difference Array is found by

$$A_1[k] = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D_k[i,j]}{M \times N} \tag{8}$$

2. A_2 is found by finding the average intensity of each frame, as

$$AvgFrame_k = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f_k(i,j)}{M \times N} \tag{9}$$

and then taking the difference between adjacent frame averages.

$$A_2[k] = AvgFrame_k - AvgFrame_{k+1} \tag{10}$$

where k= 1 to n-1, where n is the total number of frames in the video.

Both the differences hold the difference between the frame intensities and are computed for the entire video. The location of the maximum element of the array is a suspected location of forgery. It is confirmed by checking whether the maximum value under consideration is a threshold time larger than the average value of its two neighbours at each side of the array. Otherwise, it is not a forgery location. It is formulated as

$$m > threshold \times \frac{A_x[n-1] + A_x[n+1]}{2} \tag{11}$$

where m is the value at the location n of the array A_x, x is either 1 or 2. The threshold is set as 20 for A_1 and 8 for A_2 empirically. If m satisfies the above inequality, n is considered as a valid location of forgery and it is deleted from the array and the next maximum is considered and the process is repeated. Thus if two such locations are found for a video it is considered as the location of insertion and copy forgeries while for deletion forgery only one value must appear as deviating from the normal values in the difference array. If no location identified using the array A_1, then array A_2 is checked. After using both arrays if forgery doesn't get detected, the video is considered as authentic.

4.1.1 Experimental Results and Discussion

In this section, we describe the experimental analysis of the proposed Pixel-based Statistical Analysis method for video forgery detection and localization. Publicly available datasets are collected based on the requirement for experimentation and preprocessing is applied to the data to make it ready for experimentation. Frames constituting the video were extracted and converted to grayscale before carrying out further processing. The technique proposed is extensively tested using the publicly available datasets as detailed below.

Table 4: Datasets used in the experimentation for Video Forgery Detection and Localization

Name of the Dataset	**Total No. of Videos**	**Forged**	**Authentic**
VIFFD[12]	120	90	30
TDTVD Dataset[8]	226	210	16
Surveillance Video Dataset[17]	15	15	0
Inter-Frame Forgery Dataset[16]	48	32	16

Video Forgery Detection and Localization experimentation are performed using the dataset shown in Table 4. They contain varying numbers of authentic and forged videos. Videos in it are forged using copying, insertion, deletion, and shuffling.

VIFFD dataset contains 30 videos each having Copy, Insert and Delete forgeries. Surveillance Video Dataset contains 5 videos with Shuffling forgery, 5 videos with Insert forgery and 5 more videos with Delete forgery. In the TDTVD dataset the Copy, Insert and Delete forgeries are done in two different fashions. EOP(Event/Object/Person) removal or modification and ST(Smart Tampering or Multiple Tampering). EOP-based videos include 40 videos for each tampering type, frame deletion, frame duplication and frame insertion. In ST-based tampering, multiple tampering occurs in a single video. Multiple tampering is done at three different locations in the video in three categories as 10-frames tampered, 20-frames tampered, and 30-frames tampered. It contains 16 videos without any forgery. In the Inter-Frame Forgery Dataset there are a total of 48 videos out of which 16 are with no tampering, 3 videos with Copy and Shuffling, 9 videos have Shuffling forgery, 5 videos each have Delete and Insert forgery, and 10 videos with Copy forgery. The metric used for performance evaluation for video forgery detection is Accuracy. Accuracy is a measure of the correctness of a classification model. It is calculated as

$$\text{Accuracy} = \frac{\text{Number of Correct Predictions}}{\text{Total Number of Predictions}} \tag{12}$$

The proposed video forgery detection and localization approach called the Pixel-based Statistical Analysis uses a Rule-based classifier for classification. The proposed method is experimented using all the datasets listed in Table 4. Table 5 shows a comparison with a state-of-the-art method in which the delete and insert forgeries of VIFFD dataset only are considered. So the average of our results for the insert and delete forgeries for the proposed Pixel-based Statistical Analysis approach and the same using correlation coefficient as a feature are compared with the state-of-the-art. The feature based on correlation coefficient works based on the fact that the correlation coefficients of adjacent frames show similarity and hence the distance measure will have a low value for authentic videos under the assumptions made for the Pixel based Statistical

Table 5: Comparative Analysis of the proposed Video Forgery Detection and Localization Approach using VIFFD[12] dataset.

Approach	**Accuracy(%)**
Proposed Pixel-based Statistical Analysis	86.66
Proposed Correlation Coefficient based	87
Vinay et.al[10]	83

Analysis approach. A deviation from this indicates forgery. It can be seen that the correlation coefficient feature gives a slight improvement in performance for these two forgeries. Results of the experimentation for the various datasets for the proposed approach are shown in Table 6. In the case of TDTVD dataset the average accuracy for each sub category in the specified forgery type is displayed. For example, EOP forgery type depicts the average accuracy for EOP-Copy, EOP-Insert and EOP-Delete.

4.2 Proposed Inter-Frame Video Forgery Detection and Localization using Principal Component Analysis

Principal Component Analysis(PCA) is a widely used dimensionality reduction technique that can be employed for video forgery detection. PCA aims to transform high-dimensional data into a lower-dimensional space while retaining the most important information. PCA achieves this by identifying and computing new orthogonal variables, known as principal components, which are linear combinations of the original features. PCA using eigenvalues and eigenvectors is defined by:

$$\Sigma v = \lambda v \tag{13}$$

where Σ *is the Covariance matrix of the original data,* v *is the Eigenvector* and λ *is the Eigenvalue*

The covariance matrix Σ can be decomposed into the product of eigenvectors and a diagonal matrix of eigenvalues:

$$\Sigma = V \Lambda V^T \tag{14}$$

where V *is the Matrix of eigenvectors* and Λ *is the Diagonal matrix of eigenvalues*

The principal components can be obtained by projecting the centered data matrix X onto the eigenvectors:

$$Z = XV \tag{15}$$

Table 6: Accuracy of the Pixel-based Statistical Analysis approach for various forgeries for various Datasets[16]

Dataset	**Type of forgery**	**Accuracy(%)**
VIFFD	Copy	86.66
	Delete	73.33
	Insert	100
	No Forgery	70
Surveillance Video Dataset	Shuffling	100
	Delete	100
	Insert	100
TDTVD	EOP	93.99
	ST-10	90
	ST-20	93.33
	ST-30	96.66
	No Forgery	75
InterFrame Forgery Dataset	Copy	90
	Delete	100
	Insert	100
	Shuffling	77.77
	No Forgery	75

Each column of Z represents a principal component, and the proportion of variance explained by each principal component is given by the ratio of the corresponding eigenvalue to the sum of all eigenvalues. The proposed approach relies on the utilization of the foremost principal component for processing, involving the largest eigenvalue ($\lambda 1$) and the corresponding eigenvector (v1). In a video with a constant frame rate and minimal abrupt movement, PC1 exhibits a gradual pattern of change. Any sudden deviations in this pattern may indicate a potential video forgery, which is utilized for feature extraction via PCA. Despite PC1 consisting of both the eigenvalue and the corresponding eigenvector, we solely utilize the eigenvalue for feature extraction. Specifically, we compute the difference in eigenvalues between adjacent frames as a feature and each such calculated difference for all adjacent frames is stored in an array. Further, the calculated difference values are analysed and the one which deviates most from the rest of the values in the array is considered a suspected outlier. It is confirmed by checking whether its z-score exceeds a threshold. The threshold is empirically set as 3. The z-score (standard score) of an element in an array is a measure of how many standard deviations that element is away from the mean of the array. It is calculated as $z = \frac{(x-\mu)}{\sigma}$ where z is the z-score of the element, x is the value of the element to standardize, μ is the mean (average) of the array and σ is the standard deviation of the array.

If an outlier can be detected in the array the video is considered as forged. Moreover, to enhance the precision of detection, a feature based on the intensity variations among the frames is employed. In the temporal domain of the video, we anticipate a consistent change in the average intensity of each frame, while any variation may signify forgery. A block diagram depicting the proposed method is shown in Figure.12. As an initial step, the frames of the video are extracted

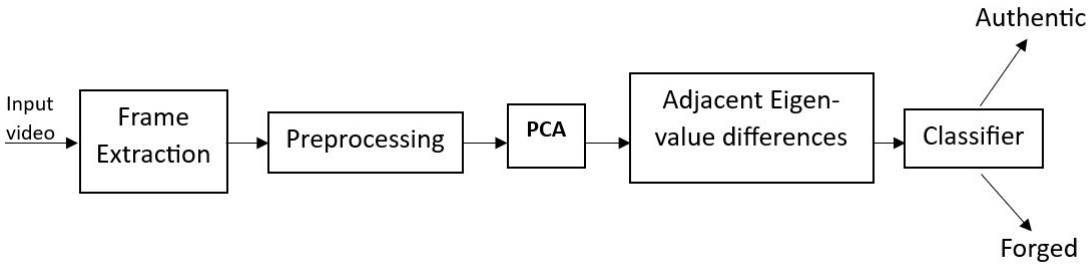

Figure 12: Block Diagram of the PCA-based Video forgery Detection

and converted to grayscale. The preprocessing necessary for PCA is performed on the frame matrix and then it undergoes PCA. The differences between the adjacent principal eigenvalues are stored in an array to find the presence of an outlier. Another array is maintained which stores the adjacent frame intensity average differences, that too is searched for an outlier in case none is detected by the use of eigenvalue differences. If an outlier is detected, the video is

classified as forged and authentic otherwise.

This approach is efficient in inter-frame video forgery detection. It has been tested using publicly available datasets and is found to perform better than many state-of-the-art methods. Applying the approach to each video segment after identifying the shot boundaries as mentioned in the previous section will improve the performance which is part of our future work.

4.2.1 Experimental Results and Discussion

In this section, we describe the experimental analysis of the proposed approach for video forgery detection and localization. The details of the datasets used in the experimentation and a description of the evaluation metrics used are the same as those mentioned in section 4.1.1.

The proposed approach uses a Rule-based classifier for classification. It is experimented using all the datasets listed in Table 4. Results of the experimentation for the various datasets for the proposed approach are shown in Table 7. In the case of TDTVD dataset the average accuracy for each subcategory in the specified forgery type is displayed as mentioned in the previous section. For example, EOP forgery type depicts the average accuracy for EOP-Copy, EOP-Insert and EOP-Delete.

In the experimental results for the approaches we proposed for Video Forgery Detection and Localization, there are clear variations in the performance of both. They have been experimented with four different datasets and generally, the Pixel-based Statistical Analysis approach seems to outperform the PCA-based method. A reason for it to outperform is that there are two thresholds empirically set in it for outlier detection even though it limits its generality. However, the PCA-based method can be considered more general as it sets the threshold to 3 irrespective of the features involved in the detection. So even though its performance compared to the other one is low, it is more general and also works better to identify the authentic videos accurately.

Thus this section described the video forgery detection and localization methods we carried out as part of the research endeavour. Both the approaches proposed are capable to carry out the task efficiently outperforming many of the state-of-the-art methods. The following section describes the contributions provided by this research work to the field of digital media forgery detection especially image and video.

5 Contributions of this Research Work

Every scientific research endeavour contributes to the field of research by developing new methods of handling the problem at hand. Our research work in digital media forgery detection provides the following contributions. Each section above describes each work and supports the below

Table 7: Accuracy of the PCA-based Approach for various forgeries for various Datasets

Dataset	**Type of Forgery**	**Accuracy(%)**
VIFFD	Forged	71.11
	Authentic	93.33
Surveillance Video Dataset	Shuffling	80
	Delete	80
	Insert	100
TDTVD	EOP	91.25
	ST-10	76.66
	ST-20	86.66
	ST-30	90
	No Forgery	81.25
InterFrame Forgery Dataset	Copy	90
	Delete	80
	Insert	100
	Shuffling	100
	No Forgery	81.25

listing.

- Utilising the fact that the vast majority of images in digital media undergo JPEG compression, we developed a technique that uses the local statistics of the DCT coefficients of the image blocks to detect forgery. Also, in this approach, we exploited the inherent learning capabilities of deep learning architecture. It provides the users with a tool for image forgery detection that they can use without worrying about the type of forgery as it works fine for any type of image forgery.

- Our work provides a valuable contribution to the field of image forgery detection by proposing a recompression-based approach. By leveraging compression artefacts, the proposed approach enhances the accuracy and robustness of forgery detection.

- Through the JPEG compression-based method for image forgery localization, our research makes a significant contribution to the field of forgery localization by introducing an innovative approach that focuses on the nuanced analysis of compression artefacts. Our method goes beyond conventional forgery detection techniques, providing a robust and precise framework for localizing manipulated regions within digital images. Through an in-depth exploration of compression artefacts, our goal is to enhance the accuracy and reliability of forgery localization approaches.

- This research presents a valuable contribution to the field of video forgery detection through a spatial intensity variation-based method. By analyzing subtle changes in spatial intensity patterns, our approach enhances the precision and effectiveness of detecting forged content within videos. The method's ability to discern spatial alterations contributes significantly to the advancement of video forensics.

- This research also presents an innovative contribution to the field of video forgery detection through the introduction of an eigenvalue difference-based method. By leveraging the distinctive characteristics of eigenvalue differences in video frames, our approach enhances the precision and effectiveness of detecting forged content within videos. The method is effective in identifying subtle alterations in the values under consideration, thus contributing to the field of video forensics.

6 Conclusion

Several works related to digital media forgery detection have been carried out in this research endeavour especially in digital images and in digital videos. Forgery detections in the image have been carried out using local 8x8 block DCT features and by exploiting the compression artefacts

in JPEG compression. Both methods are found to exhibit significant performance improvement over the existing ones. Video forgery detections have been performed using Spatial Intensity Variations and eignen-value differences as features. These methods too have been found to perform better than many of the existing ones. Many existing challenges have been overcome by the proposed approaches. The tremendous power of deep learning models in classification has been explored in this work. The works carried out by several other researchers have motivated us to do further research and come out with new findings in this area. This arena of research prompts us to do more work on the current and related topics and come out with better results in the future.

Publications:

1 **Local DCT-Based Deep Learning Architecture for Image Forgery Detection.**

Authors: B H Shekar, Wincy Abraham, Bharathi Pilar

Publication date: 06-05-2023

Conference: Computer Vision and Machine Intelligence

BookTitle: Lecture Notes in Networks and Systems

Volume: 586

Pages: 465-473

Publisher: Springer

2 **Image Forgery Detection: A re-compression based Approach**

Authors: B H Shekar, Wincy Abraham, Bharathi Pilar

Publication date: Communicated

Journal: Springer Nature Computer Science

Volume:

Pages:

Publisher:

3 **A JPEG compression-based method for Image Forgery Localization**

Authors: B H Shekar, Wincy Abraham, Bharathi Pilar

Publication date: To be Communicated

Journal:

Volume:

Pages:

Publisher:

4 **Simple Difference Based Inter Frame Video Forgery Detection And Localization,**

Authors: B H Shekar, Wincy Abraham, Bharathi Pilar

Publication date: 12/02/24

Conference: Fifth International Conference on Computing and Network Communications

BookTitle: Lecture notes in Electrical Engineering

Pages: 3-14

Publisher: Springer

5 **Inter-Frame Video Forgery Detection - A PCA-Based Approach**

Authors: Wincy Abraham, B H Shekar, Bharathi Pilar

Publication date: Publishing Soon

Conference: Fifth International Conference on Computing and Network Communications

BookTitle: Lecture notes in Electrical Engineering

Pages:

Publisher: Springer

References

[1] Ganapathi I.I. Vu N.-S. Ali S.D. Saxena N. Werghi N. Ali, S.S. Image forgery detection using deep learning by recompressing images. *Electronics*, 11(403), 2022.

[2] Gao T. Fan L.-Yang Q. Cao, Y. A robust detection algorithm for copy-move forgery in digital images. *Forensic science international*, 214(33):1–3, 2012.

[3] Jing Dong, Wei Wang, and Tieniu Tan. CASIA image tampering detection evaluation database. In *2013 IEEE China Summit and International Conference on Signal and Information Processing*. IEEE, 2013.

[4] Singh J. Parthasarathy H Dua, S. Image forgery detection based on statistical features of block dct coefficients. *Procedia Computer Science*, 171:369–378, 2020.

[5] Qadir F. Gani, G. A robust copy-move forgery detection technique based on discrete cosine transform and cellular automata. *Journal of Information Security and Applications*, 54(102510), 2020.

[6] Wang W Farid H. Exposing digital forgeries in video by detecting duplication. In *Proceedings of the 9th Workshop on Multimedia and Security - MM Sec '07*, 2007.

[7] Zhang Z. Yang S.-Xie D. Pu S. Hao, J. Transforensics: Image forgery localization with dense self-attention. *ArXiv. /abs/2108.03871*, 2021.

[8] Panchal Dr. Hitesh Shah. Hitesh, D. Tdtvd -video tampering dataset development in temporal domain for video forgery authentication. *Multimedia Tools and Applications*, 79:24553–24577, 2020.

[9] N. Hoose. Computer vision as a traffic surveillance tool. *Control Computers Communications in Transportation*, pages 57–64, 1990.

[10] Gaur M. Kumar, Vinay. Multiple forgery detection in video using inter-frame correlation distance with dual-threshold. *Multimed Tools and Applications*, 81:43979–43998, 2022.

[11] Huang J. Qiu G. Luo, W. Jpeg error analysis and its applications to digital image forensics. *IEEE Trans. Inf. Forensics Secur.*, 5:480–491, 2010.

[12] Hu J. Nguyen, XH. Viffd - a dataset for detecting video interframe forgeries. *Mendeley Data*, 2020.

[13] Sanika Patankar, Ashutosh Joshi, Gaurav Durge, Atharva Jaid, Khomesh Kalambe, and Hrishikesh Dhale. Image forgery detection using ela and cnn. In *2023 2nd International Conference on Futuristic Technologies (INCOFT)*, pages 1–7, 2023.

[14] Meet Patel, Kartikay Rane, Niyati Jain, Praneel Mhatre, and Shree Jaswal. Image forgery detection using cnn. In *2023 3rd International Conference on Intelligent Technologies (CONIT)*, pages 1–4, 2023.

[15] Nam Thanh Pham, Jong-Weon Lee, Goo-Rak Kwon, and Chun-Su Park. Hybrid image-retrieval method for image-splicing validation. *Symmetry*, 11(1):83, 2019.

[16] Qi Han. Li Qiong. Sondos, Fadl. Exposing video inter-frame forgery via histogram of oriented gradients and motion energy image. *Multidimensional Systems and Signal Processing*, 31:1365–1384, 2020.

[17] Qi Han. Qiong Li. Sondos, Fadl. Surveillance video authentication using universal image quality index of temporal average. In *17th International Workshop IWDW 2018 Jeju Island Korea*, 2018.

[18] Thampi S.M. Vidyadharan, D.S. Digital image forgery detection using compact multi-texture representation. *J. Intell. Fuzzy Syst.*, 2017.

[19] Sowmya K.N Basavaraju H.T Lohitashva B.H Chennamma H.R Aradhya V.N.M. Similarity analysis of residual frames for inter frame forgery detection in video. In *Advances in Intelligent Systems and Computing*, 2019.

[20] Chen Y. Zhou J. Wu, H. Rethinking image forgery detection via contrastive learning and unsupervised clustering. *ArXiv. /abs/2308.09307*, 2023.

[21] Morariu V Davis L Zhou P, Han X. Learning rich features for image manipulation detection. In *2018 IEEE/CVF conference on computer vision and pattern recognition*, 2018.

Research Candidate:

Wincy Abraham,
Research Scholar,
Department of Computer Science,
Mangalore University

Research Supervisor:

Dr. B.H. Shekar,
Professor,
Department of Computer Science,
Mangalore University